

REMARKS

This Request for Continued Examination after Final is filed in response to a Final Office Action of January 22, 2010 in which claims 129-182 were rejected and in response to Advisory Action of March 22, 2010 in response to a Request for Reconsideration after Final filed on February 17, 2010.

Independent claims 129, 148 and 166 are amended to make a difference between a subject matter recited in claims 129, 148 and 166 and disclosure of Wiley et al. even more distinct which is further discussed herein. Also claims 136, 159 and 172 are amended to obviate rejection under 35 USC 112, first paragraph.

\*\*\*

***Claim Rejections - 35 USC § 112***

**Examiner's Position:**

Claims 136, 159 and 172 are rejected under 35 USC 112, first paragraph, as failing to comply with the written description requirement. These claims recite "an index indicating how to enter .... Transmission event unabridged" which is not described in the specification.

**Applicant's Response:**

The Applicant continues to disagree with the Examiner. In addition to arguments presented in the Request for Reconsideration after Final filed on February 17, 2010, the Applicant would like to refer to the last paragraph on page 11 of the originally filed patent application, which further clarifies the subject matter of claims 136, 159 and 172 as being interpreted by a person skilled in the art.

However, in spite of the disagreement with the Examiner's point of view, in order to advance the prosecution, the Applicant amended claims 136, 159 and 172, as submitted herein, following Examiner's recommendation in the Advisory Action of

February 24, 2010 "to utilize language clearly supported in the originally filed specification."

\*\*\*

***Claim Rejections - 35 USC § 103***

**Examiner's Position:**

Claims 129-135, 137-140, 142-145, 148-154, 156-158, 160-171, 173-176 and 178-179 are rejected under 35 U.S.C. 103(a) as being unpatentable over Khanokar et al. (U.S. Patent No. 6560443) in view of Wiley et al. (US 7382756).

Claims 141, 155 and 177, are rejected under 35 U.S.C. 103(a) as being unpatentable over Khanokar et al. in view of Wiley et al. as applied to claims 129, 148 and 166 and further in view of Richards et al. (US 2005/0015461).

Claims 146, 147, 181 and 182 are rejected under 35 U.S.C. 103(a) as being unpatentable over Khanokar et al. as applied to claims 129, 148 and 166 and further in view Microsoft Computer Dictionary, 5th Edition.

**Applicant's Response:**

The Applicant is of opinion that some Examiner's arguments are inaccurate. The Examiner's arguments are analyzed based on MPEP guidelines which are stated in the MPEP Paragraph 2143 as follows:

"To establish a *prima facie* case of obviousness three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations.

The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, not in Applicant's disclosure. ***In re Vaeck***, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991)."

In reference to independent claim 129 (and other independent claims) of the present patent application, the Examiner admitted that Khanokar et al. did not show all features of a second step in claim 129 but further stated that Wiley et al. disclose the second step of claim 129 (before amending claim 129 as submitted herein):

"creating one or more characterization records for at least one data structure of said one or more data structures, one or more transmission events of said plurality of the transmission events being collected to said at least one data structure of said one or more data structures, wherein at least one of said one or more characterization records comprises one or more indicators of a location or locations of one or more data elements comprised in at least one of said one or more transmission events, to allow accessing said at least one of the one or more characterization records to determine said one or more indicators of the location or locations of said one or more data elements."

In addition to the arguments presented in the Request for Consideration after Final filed on February 17, 2010, the Applicant would like to make a few further remarks.

The information stored by Wiley et al. is only routing information or packet data which include only "a source IP address, a source port, a destination IP address and a destination port" (e.g., col. 4, lines 26-28 Wiley et al.). Nothing in the disclosure of Wiley et al. indicates that any of the originally received transmission event data comprising substantive content of the message is saved (except routing

information or packet data, as pointed herein), which makes sense, because Wiley et al. do not need to save any originally received "substantive" data since the "problem to be solved" by Wiley et al. is not to get access to the originally received substantive data (which is one problem solved by the present patent application) but to detect intrusion network activity, and for that purpose, only data representative comprising routing information or packet data (in order to generate a "signature") is needed and therefore stored in datasets which include keysets (e.g., see col. 4 lines 18-30 and ABSTRACT of Wiley et al.).

On the other hand, one or more data elements (which is apparently saved and which location or locations are comprised as one or more indicators in one of said one or more characterization records) recited in claim 129 (and other independent claims) of the present patent application have much broader definition. It is well known to a person skilled in the art that "data element" of a transmission event may be any original data comprised in the transmission event, e.g., routing information (e.g., IP address of a node), and a substantive content (e.g., a message content, title/subject of the message, etc.). There is no any limitation in the disclosure of the present patent application in regard to what part of the original (or raw) data or data elements of the transmission event may be captured and saved. On the contrary, it is stated in the disclosure of the original patent application (e.g., see page 11, lines 14-17): "It should be appreciated that, although there may be diagnostic benefits to loading network event notifications in their entirety to storage, the invention is obviously not limited in this regard. Any suitable portion of a notification, up to and including an unabridged version, may be loaded to storage." This broad statement means that any portion

of the transmission event, e.g., routing information (e.g., IP address of a node), and/or a substantive content (e.g., a message content, title/subject of the message, etc.) may be saved (e.g., loaded to storage) as one or more data elements.

Therefore, in order to further distinguish the subject matter recited in claim 129 and other independent claims and the disclosure of Wiley et al., claim 129 (as well as claims 148 and 166) is amended to include a clarification (underlined and bolded) that "one or more data elements stored in said one or more data structures and comprising a substantive content or a message comprised in at least one of said one or more transmission events". This clarification is fully supported by the disclosure of the present patent application as explained herein.

Therefore, none of the references (Khanokar et al. or Wiley et al.) quoted by the Examiner teach or disclose a second step of claim 129 quoted herein, especially after being amended as submitted herein, such that none of these references disclose all limitations of claim 129, as required by the MPEP Paragraph 2143 quoted herein, which makes claim 129 non-obvious and not unpatentable over Khanokar et al. in view of Wiley et al. under 35 U.S.C. 103(a), contrary to what is alleged by the Examiner.

Moreover, incorporating teaching of Wiley et al. into Khanokar et al. will teach away from the subject matter recited in claim 129 (and other independent claims) because Wiley et al. do not teach storing a substantive content/message in the data structures, as emphasized in the amendment submitted herein.

Furthermore, in regard to claim 129 of the present invention, the Office failed to show prima facie case of obviousness and demonstrate or provide convincing arguments in regard to "suggested desirability or motivation" or "reasonable expectation of success" (no arguments made at all)

for combining references by a person skilled in the art at the time of the invention without the benefit of hindsight (assuming for sake of argument only that quoted references teach or suggests all the limitations of independent claim 129), as required by MPEP paragraphs 2143 (quoted above) and 2142, and by an extensive case law on the subject quoted above.

Indeed, if we assume for the sake of argument only that Khanokar et al. and Wiley et al. disclose all steps and limitations of claim 129 of the present patent application (which is not the case as shown herein), the Examiner did not show convincingly that the quoted references contain suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to combine reference teachings to arrive at the subject matter of claim 129 (and other independent and dependent claims) of the present invention without the benefit of hindsight.

On page 6 (top paragraph) of the Final Office Action of January 22, 2010, the Examiner stated that "It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Khanokar et al. with that of Wiley in order to provide faster access to stored data (Wiley, col. 2, lines 17-28)". The Applicant disagrees with the Examiner. Indeed, someone may ask a question: "faster" relative to what? The problem to be solved by both inventions of Khanokar et al. and Wiley et al. is related to providing security (e.g., detecting network intrusion events as evident from ABSTRACTS of both patent applications). Then the Examiner's reference to col. 2 lines 17-28 of Wiley et al. to provide justification for combining references of Khanokar et al. and Wiley et al. is not convincing because it is stated in col. 2 lines 17-19 of Wiley et al. that "Technical advantages of the present patent

application include providing an improved method and system for maintaining network activity data for intrusion detections, ...." Nothing is indicated in col. 2 lines 17-28 of Wiley et al. about "providing faster access to stored data" than by the system of Khanokar et al. (without creating characterization records) or by other known systems utilizing creating characterization record as recited in claim 129. The datasets with keysets and pointer system disclosed by Wiley et al. is for creating a signature for intrusion detection, as discussed herein.

Nothing in Wiley et al. indicates that this datasets/keysets/pointer system of Wiley et al. will be faster than the system disclosed by Khanokar et al. for detecting an intrusion event or any other system from relevant art. In other words, it would not be clear to a person skilled in the art at the time of the present invention from the disclosures of Wiley et al. and Khanokar et al. or other known techniques, e.g., for creating characterization records, what would be the benefit for adding a rather complex data storage system comprising datasets/keysets/pointer system of Wiley et al. to the teaching of Khanokar et al. in order to provide, according to claim 15 of the present patent application, that "at least one of said one or more indices comprises one or more indicators of a location or locations of one or more data elements stored in said one or more data structures and comprising a substantive content or a message comprised in at least one of said one or more transmission events".

In the Advisory Action of February 24, 2010, the Examiner continued to argue that the teaching of Wiley et al. may improve managing network traffic by reducing the number of searches required for reoccurrence of the network traffic and/or occurrence of related network traffic (Wiley et al. col. 2 lines

25-28). Again, "reducing a number of searches" relative to what?

In general, reducing a number of searches can make the process faster or slower depending on how long the "one" search is. Again, there is no indication in Wiley et al. that the number of "searches" is reduced relative to the procedure disclosed by Khanokar et al. or other known techniques and that the "search" process in Wiley et al. is faster (again relative to what?).

Moreover, the problem to be solved by the present application is to provide capturing for storing and maintaining files on the site in a certain way such that this stored data can be effectively recovered (no emphasis on the speed). In other words, the emphasis is on the methodology of retaining data and creating appropriate characterization records in order to recover the desired data and not on maintaining network activity data for intrusion detection with a minimum number of searches as stated by Wiley et al. and "higher speed" as alleged by the Examiner (again number of searches and/or speed is a relative term, i.e. relative to what?).

In other words, the Examiner's reasoning for incorporating Wiley et al. into Khanokar et al. to arrive at the subject matter of claim 129 is practically similar to "shared advantage" approach such as achieving competitive advantage or economical advantage (which can make any invention obvious) irrelevant to the "problem to be solved" by the present invention.

The Manual of Patent Examining Procedure (the MPEP) clearly refers to the "problem to be solved" approach and cites a relatively recent Federal Circuit case supporting its use: "The test for an implicit showing is what the combined teachings, knowledge of one of ordinary skill in the art, and the nature of the problem to be solved as a whole would have suggested to those of ordinary skill in the art." *In*

*re Kotzab*, 217 F.3d 1365, 1370, 55 USPQ2d 1313, 1317 (Fed. Cir. 2000). See also *In re Lee*, 277 F.3d 1338, 1342-44, 61 USPQ2d 1430, 1433-34 (Fed. Cir. 2002) (discussing the importance of relying on objective evidence and making specific factual findings with respect to the motivation to combine references); *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988); *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). MPEP 2143.01.

This further reinforce the conclusion that claim 129 is not unpatentable under 35 U.S.C. 103(a) over Khanokar et al. in view of Wiley et al., as stated herein.

Independent claims 148 and 166 have a similar scope as claim 129 and therefore also not unpatentable over Khanokar et al. in view of Wiley et al. under 35 U.S.C. 103(a).

The non-obviousness and patentability of dependent claims 130-147, 149-165 and 187-182 is provided by novelty and non-obviousness of the independent claims 129, 149 and 166 they are dependent from (directly or indirectly). More arguments in reference to unique limitations of dependent claims 130-148, 150-165 and 187-182 may be presented by the applicant if requested by the Office.

\*\*\*

**CONCLUSION**

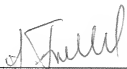
The objections and rejections of the Final Office Action of February 24, 2010 and advisory action of March 22, 2010, having been obviated by amendment or shown to be inapplicable, withdrawal thereof is requested and passage of all claims to issue is earnestly solicited.

Respectfully submitted,

**KELLEY DRYE & WARREN LLP**

Attorneys and Agents for Applicants

Date: April 20, 2010



\_\_\_\_\_  
Anatoly Frenkel

Reg. No. 54,106

400 Atlantic Street

Stamford, CT 06901

Direct Tel.: 203-351-8078

Facsimile: 203-327-2669

e-mail: [afrenkel@kelleydrye.com](mailto:afrenkel@kelleydrye.com)

**Customer No. 47670**